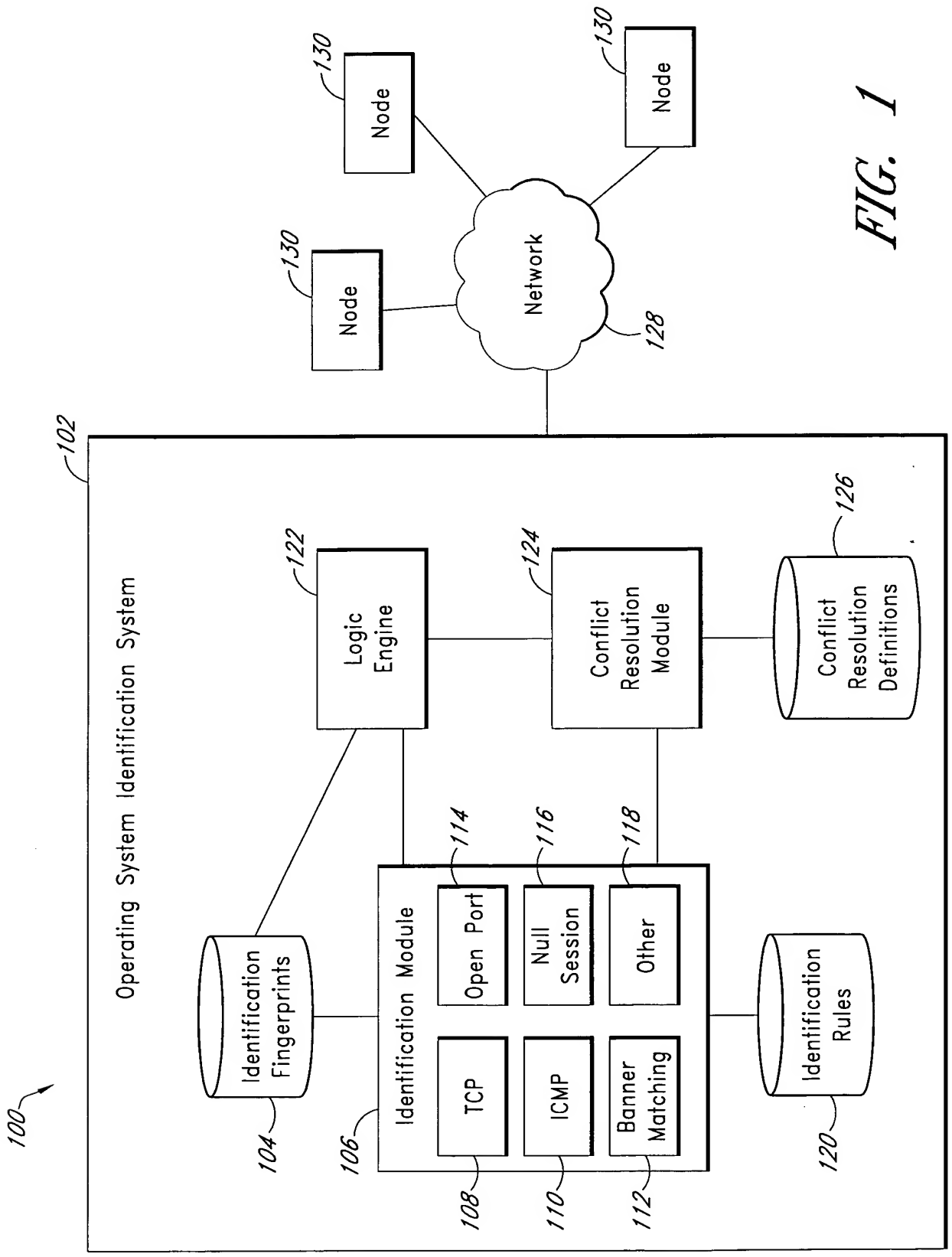
100
102
Operating System Identification System
Node
130
Node
130
Node
130
Network
128
Logic Engine
122
Conflict Resolution Module
124
Conflict Resolution Definitions
126
Identification Fingerprints
104
Identification Module
106
Open Port
114
Null Session
116
Other
118
TCP
108
ICMP
110
Banner Matching
112
Identification Rules
120

FIG. 1

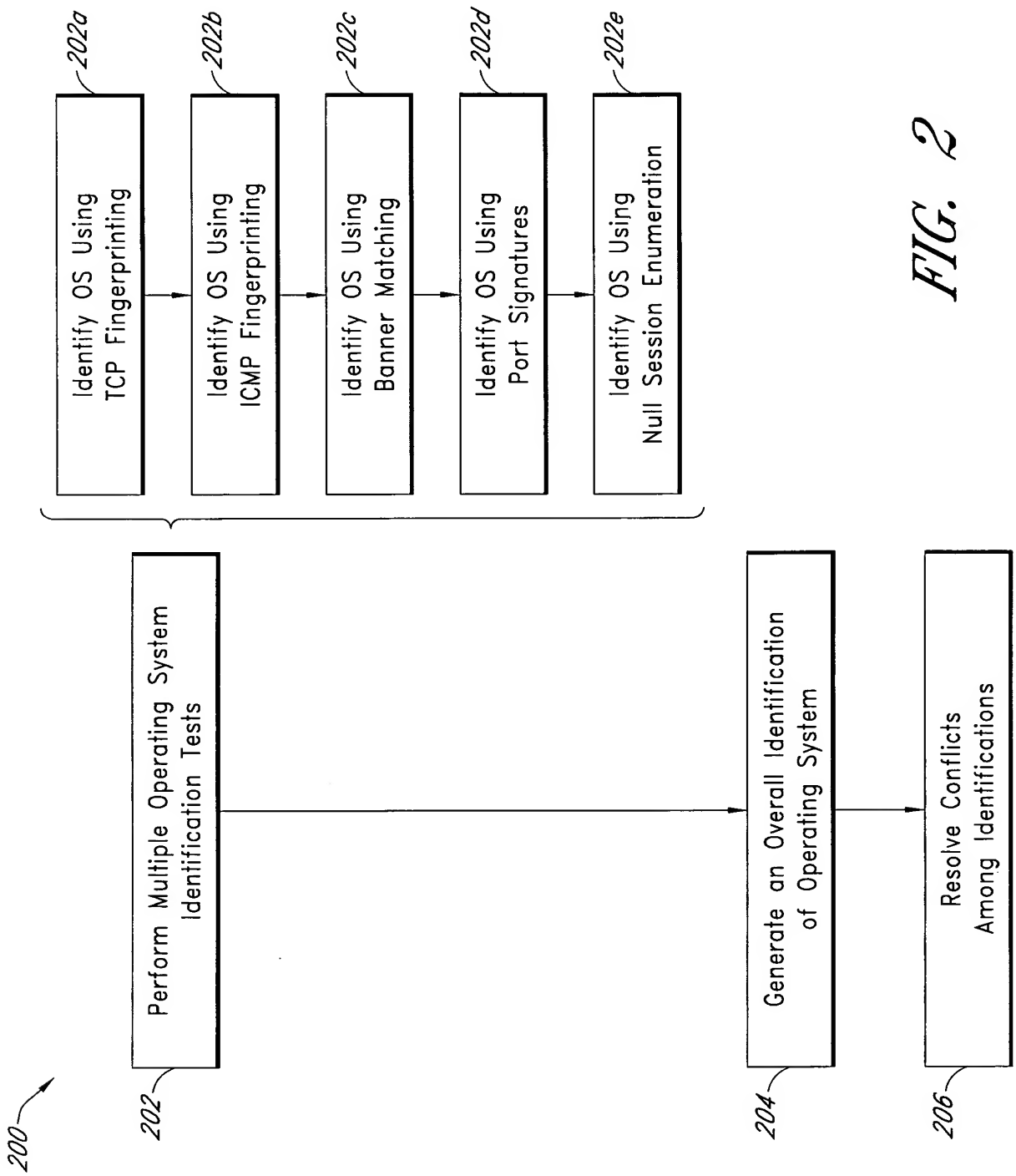
200
202
Perform Mulfiple Operating System Identification Tests
202a
Identify OS Using TCP Fingerprinting
202b
Identify OS Using ICMP Fingerprinting
202c
Identify OS Using Banner Matching
202d
Identify OS Using Port Signatures
202e
Identify OS Using Null Session Enumeration
204
Generate an Overall Identification of Operating System
206
Resolve Conflicts Among Identifications

FIG. 2

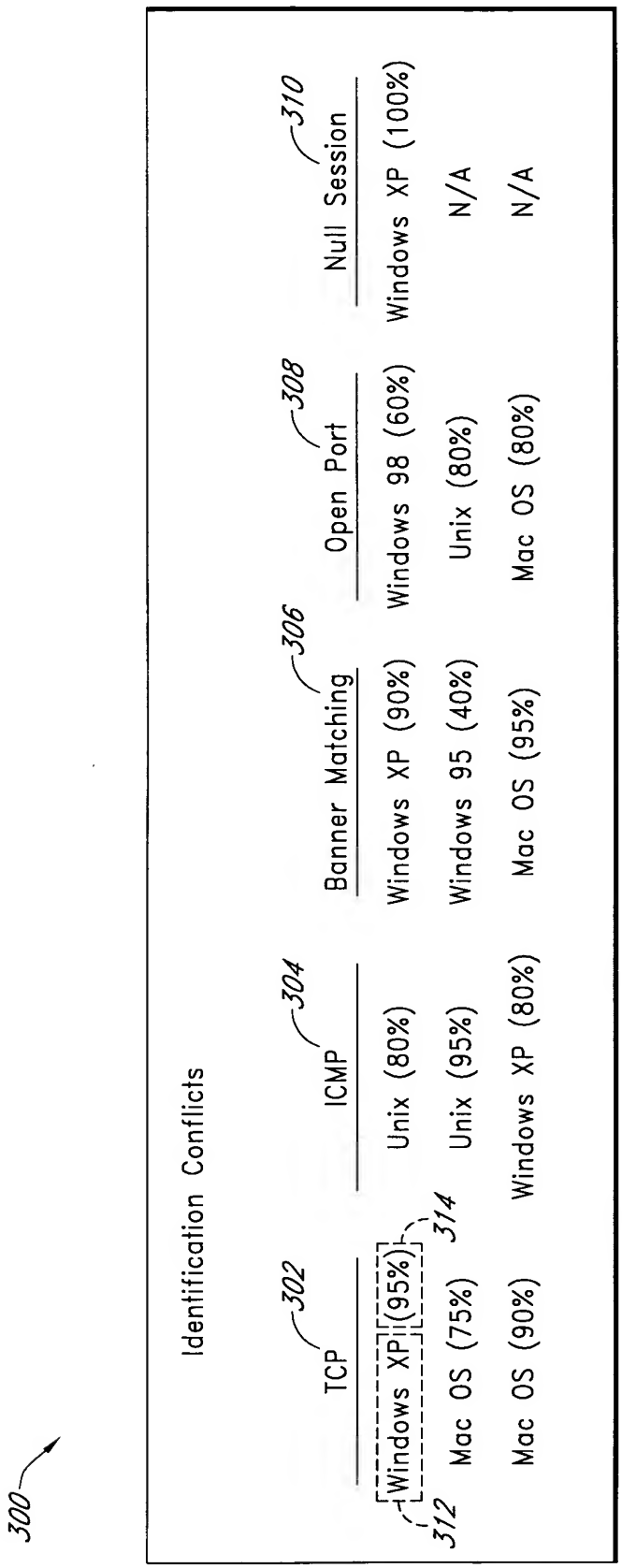
300
Identification Conflicts
TCP
302
ICMP
304
Banner Matching
306
Open Port
308
Null Session
310
Windows XP (95%)
312
314
Mac OS (75%)
Unix (80%)
Windows XP (90%)
Windows 98 (60%)
Windows XP (100%)
Mac OS (90%)
Unix (95%)
Windows 95 (40%)
Unix (80%)
N/A
Mac OS (90%)
Windows XP (80%)
Mac OS (95%)
Mac OS (80%)
N/A

FIG. 3

400
Conflict Resolution Definitions

402 TCP Fingerprint	404 ICMP Fingerprint	406 TCP Ports	408 UDP Ports	410 TCP Port & Banner	412 UDP Port & Banner	414 OS Description	416 OS Code
T40E8:4100:4080:0586:0:80:0001:1:0:MNWNNTNNS	I0001303	139, -445	137	—	—	Windows 2000	OS_Win2000
T8000:80BC:8154:05B4:0:40:0001:1:1:MNWNNT	I00017913	—	—	—	—	OS X	OS_MAC
T2000:2000:2000:05B4:0:40:0001:0:0:MNW	I00137993	—	—	—	—	Xerox Phaser 7300	OS_PRINTER
T4000:4100:4080:05B4:4:40:0001:1:1:MNWNNT	I0013793	—	—	—	161: BIG/ip	FreeBSD	OS_BSD

FIG. 4